REMARKS

Reconsideration and allowance are respectfully requested.

The IDS filed on April 29, 2005 has not been formally acknowledged by the Examiner. Applicants respectfully request consideration and acknowledgement.

Claims 47, 48, 51-54, 58-64, 66, 67, 69-71, 73, and 75 stand rejected for obviousness under 35 U.S.C. §103 based on EP 1081891 to Hopkins in view of newly-applied Wood and Fujimoto. This rejection is respectfully traversed.

Paragraph [0032] of Hopkins teaches a security module 24 with a secure section 26 and an unsecured section 28. For the internally confined device specific security data, the Examiner points to paragraph [0039] in Hopkins and the private part/key KPVSS which remains within the target secure section 26 and is not communicated outside the target secure section 26. The Examiner admits that Hopkins does not explicitly disclose that the device-specific security data (1) is temporarily generated, (2) is generated by performing cryptographic processing on at least partially the stored secret and received external data, and (3) can only be generated as long as external data is available at the receiver. To this list, Applicants also add that the Examiner does not identify what in Hopkins corresponds to the stored random secret recited in the independent claims. Those claims specify that the device-specific security data and the random secret are different. If the external data in Hopkins is the SSID from the MIF 110 and the device-specific security data in Hopkins is the private key, it is unclear what would reasonably viewed as the stored random secret in Hopkins.

Applicants also observe that Hopkins's generates the public key pair in the secure section SS 126 using internal data only. The external data (SSID) form the MIF 110 is not used in the key generation. In other words, Hopkins lacks the claimed "externally received trigger data from

the user to generate a temporarily available instance of the device-specific security data internally confined within said electronic circuit during usage of said device," as recited in claim 47.

Wood discloses enhancing entropy in a pseudo-random number generator. The apparatus depends on internal provisioning of random number and on external servers of random numbers. By relying on several external servers, Wood's arrangement is more secure against attempts to guess a random number that is input to PRNG for generation of a key.

Fujimoto discloses a tamper proof microprocessor for protecting secrets of programs. The processor loads initially a program encrypted by a public key associated with the processor. The processor may decrypt the program using its corresponding secret key; whereafter, the clear text program may start executing. An interrupt may cause ongoing processor execution to stop to load a new task. At this instance, the processor may save register contents to an external memory so that execution of the original program may later restart. To protect the saved data from unauthorized tampering, the processor generates a random number to creation a cryptographic symmetric key for encrypting the register data prior to saving it on the external memory. The random number is calculated from randomly varying data at the processor such as voltage variations. That key is later re-used to decryption the data when it is re-loaded into processor from the external memory for continued program execution.

Even if these three references could be combined for purposes of argument only, they do not teach all the features recited in the independent claims. For example, that combination does not teach the "storage device for tamper-resistantly storing, during manufacture of the tamper-resistant electronic circuit, a random secret not accessible over any external circuit interface to the tamper-resistant electronic circuit" in addition to the claimed trigger data and the claimed

device-specific security data. Nor do any of the references teach "trigger data generating circuitry for, during configuration of the tamper-resistant electronic circuit, generating trigger data using the random secret and device-specific security data that is different from the random secret and outputting the trigger data outside of the tamper-resistant electronic circuit" followed in operation by "a cryptographic processing engine, in response to the externally received trigger data from the user, for performing cryptographic processing at least partly in response to said stored secret and the externally received trigger data from the user to generate a temporarily available instance of the device-specific security data internally confined within said electronic circuit during usage of said device."

Neither Wood nor Fujimoto describe the manner in which the trigger data (e.g., see the trigger data X in non-limiting, example embodiment in Fig. 6 in the instant application) is generated at the device at manufacturing using (1) the secret (e.g., see the secret C in non-limiting, example embodiment in Fig. 6 in the instant application) and (2) the device specific security data (e.g., see the encryption key K in non-limiting, example embodiment in Fig. 6 in the instant application) and then provided to an operator or user for subsequent use. Nor do any of the applied references teach that later, in use, a cryptographic processing engine, in response to the externally received trigger data from the user, performs cryptographic processing using the stored secret and externally-applied trigger data from the user in order to generate a temporarily available instance of the device-specific security data that stays internally confined within said electronic circuit during use. A significant advantage of this approach is that the device specific security data itself (e.g., see the encryption key K in non-limiting, example embodiment in Fig. 6 in the instant application) never need be supplied during use. The device specific security data (e.g., see the encryption key K in non-limiting, example embodiment in Fig. 6 in the instant

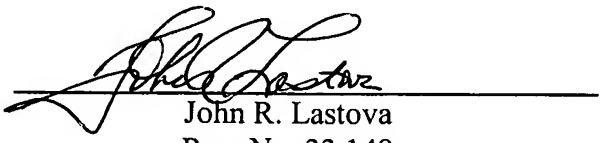
application) is generated on the fly totally internal to the tamper-resistant circuit. In Hopkins, the device specific data corresponding to the private key appears to remain fixed because the cryptographic process for generating the private key is not re-run. Wood does not disclose generating an instance of security data using external data as claimed because once sufficient external random data has been acquired, the internal PRNG may produce security data and the external random data input may be cut off.

For the reasons explained above, the obviousness rejection should be withdrawn. If the Examiner elects to make any further prior art rejection, the Examiner is requested to specifically identify in the prior art references what information in each reference corresponds to the claimed random secret, trigger data, device-specific security data that is different from the random secret, the manufacturing/configuring operations, the use operation, and the temporarily available instance of the device-specific security data.

The application is in condition for allowance. An early notice to that effect is requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 

John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100